EQUIVALENCE CLASSES OF PRIMITIVE BINARY QUADRATIC FORMS AND ZETA FUNCTIONS

数理解析研究所講究録
第 797 巻 1992 年 110-125

EQUIVALENCE CLASSES OF PRIMITIVE BINARY QUADRATIC FORMS AND ZETA FUNCTIONS

PIA BAUER

Department of Mathematics
Faculty of Science
Kyushu University 33
Higashi-ku, Fukuoka 812, Japan

December 1991

0. INTRODUCTION

For an arbitrary number field $\mathbf{K}$ with ring of integers denoted by $\mathcal{O}$ we study $\mathrm{GL}(2,\mathcal{O})$ (=:G)– and $\mathrm{SL}(2,\mathcal{O})$–equivalence classes of binary quadratic forms $\Phi(x,y)=ax^2+bxy+cy^2$ defined over $\mathcal{O}$. After fixing $\Delta\in\mathcal{O}$ we define the following zeta function for G–equivalence classes of the binary quadratic forms over $\mathcal{O}$ of discriminant Δ:

$$P_\Delta(s):=\sum_{\substack{[\Phi]\\ \Phi\text{ primitive}\\ \Delta(\Phi)=\Delta}}\ \sum_{(x,y)\in(\mathcal{O}\times\mathcal{O})/\mathrm{E}(\Phi)}|\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\Phi(x,y))|^{-s},\ \Delta\neq\text{square},$$

where $\mathrm{E}(\Phi):=\{g\in\mathrm{G}:g\Phi=\Phi\}$.

For the rational numbers and imaginary quadratic fields one can define this also for $\mathrm{SL}(2,\mathcal{O})$–equivalence, which for convenience we call 1–equivalence.

We will express it in closed form in terms of the zeta function of an order in the field $\mathbf{L}=\mathbf{K}(\sqrt{\Delta})$ associated to the primitive forms. For the latter one can also find a description by L–series of $\mathbf{L}=\mathbf{K}(\sqrt{\Delta})$. The simplest method to give an identity involving L–series would be to take a representing form of each class, represent it as norm form of the associated module in the extension $\mathbf{L}$ of $\mathbf{K}$ by $\sqrt{\Delta}$ and employ the module zeta function in [Od]. Since each module has a different conductor this does not lead to a closed form. But with this method one can omit the restriction to primitive forms, i.e. the ideal generated by the coefficients of the form is $\mathcal{O}$. For primitive forms the corresponding modules all have the same endomorphism ring R and their similarity classes form a subgroup of the ideal class group of R. This leads to the desired description of $P_\Delta(s)$ (Theorem 5.9).

In the first paragraph we give the basic definitions. In §2 we extend the concept of pairs introduced in [Ka1] for $\mathrm{SL}(2,\mathcal{O})$–equivalence to G–equivalence and prove for given discriminant the 1–1–correspondence between G–equivalence classes of pairs and G–equivalence classes of binary quadratic forms (Lemma 2.2). In §3 we study the automorphism group of a form. Using the description of G– and $\mathrm{SL}(2,\mathcal{O})$–equivalence classes of pairs, the correspondence (Lemma 2.2) and the description of the automorphism group we show that the G–equivalence class of a form Φ splits into $[\mathcal{O}^* : N(\mathcal{O}_\Phi^*)]$ many $\mathrm{SL}(2,\mathcal{O})$–equivalence classes, $\mathcal{O}_\Phi$ denotes the endomorphism ring of the associated module (Lemma 3.2). In §4 we study the structure of the endomorphism ring $\mathcal{O}_A$ of a module A coming from a binary quadratic form. We show that it is free over $\mathcal{O}$ if and only if the coefficients of the form generate a principal ideal in $\mathcal{O}$. Fixing $\mathcal{O}_A$ we see that the finitely generated modules over $\mathcal{O}$ in $\mathcal{O}_A$ which have $\mathcal{O}_A$ as endomorphism ring (called 'proper') are exactly the $\mathcal{O}_A$–regular ideals which are characterized by the existence of a similar ideal which is coprime to the conductor of $\mathcal{O}_A$ in the integral closure of $\mathcal{O}$ in $\mathbf{L}$. With this characterisation one can construct a map from the ideal class group of $\mathcal{O}_A$ to the ideal class group of $\mathbf{K}$ which is a homomorphism if and only if $\mathcal{O}_A$ is free over $\mathcal{O}$ (Lemma 4.11). Its kernel is generated by the classes of free (over $\mathcal{O}$) proper modules of $\mathcal{O}_A$. In §5 we gather the results so far to show an 1–1–correspondence between G–equivalence classes of binary quadratic forms over $\mathcal{O}$ of discriminant Δ ($\neq$ square) and similarity classes of free (over $\mathcal{O}$) proper modules of the unique oder of discriminant Δ that is free over $\mathcal{O}$. We show

$$P_\Delta(s) = Q_\Delta(s) := \sum_{\substack{A \subset R,\ \text{proper ideal} \\ \text{free over } \mathcal{O}}} \mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\mathrm{N}(A))^{-s}.$$

In §6 we identify $Q_\Delta(s)$ as indicated in the beginning (Theorem 6.1) and by this give the analytic continuation of $P_\Delta(s)$.

1. Equivalence of binary quadratic forms

Let $\mathbf{K}$ be an algebraic number field, $\mathcal{O}$ its ring of integers. For $a, b, c \in \mathcal{O}$ define the binary quadratic form

$$\Phi(x,y) = ax^2 + bxy + cy^2.$$

It has discriminant $\Delta(\Phi) = b^2 - 4ac$. We can assign the symmetric matrix $A = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$ to Φ and write $\Phi(x,y) = (x,y)A(x,y)^t$.

On such a form the 2×2–matrices with integral coefficients operate by

$$\begin{aligned}[g]\Phi(x,y) := \Phi((x,y)g) =&(x,y)gAg^t(x,y)^t, \qquad g = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \in \mathrm{M}(2,\mathcal{O}),\\ =&a'x^2 + b'xy + c'y^2\end{aligned}$$

with

$$\begin{aligned} a' =& a\alpha^2 + b\alpha\gamma + c\gamma^2 = \Phi(\alpha,\gamma) \\ b' =& 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta \qquad (1.1) \\ c' =& a\beta^2 + b\beta\delta + c\delta^2 = \Phi(\beta,\delta). \end{aligned}$$

The discriminant behaves under this operation like $\Delta([g]\Phi) = \det(g)^2\Delta(\Phi)$.

We want to study zeta functions associated to equivalence classes of binary quadratic forms of a fixed discriminant. For this we introduce the following equivalence relation. We fix $\Delta \in \mathcal{O}$ and set $G := \mathrm{GL}(2, \mathcal{O})$.

1.1. Definition. *We call two binary quadratic forms Φ and Ψ over $\mathcal{O}$ of discriminant Δ G–equivalent if there exists an element $g \in \mathrm{G}$ such that*

$$(g\Phi)(x, y) := \det(g)^{-1}\Phi((x, y)g) = \Psi(x, y).$$

If we only allow transformations of determinant 1, *we call the forms 1–equivalent.*

This is in fact an equivalence relation. Two equivalent forms represent up to a unit the same numbers.

$$\mathrm{E}(\Phi) := \{g \in \mathrm{G} : g\Phi = \Phi\} \quad \text{and} \quad \mathrm{E}_1(\Phi) := \{g \in \mathrm{G} : g\Phi = \Phi \ \det g = 1\} \tag{1.2}$$

are the groups of G–automorphisms and 1–automorphisms of Φ.

The numbers h_{G} and h_1 of G– and 1–equivalence classes for a given discriminant $\Delta \neq 0$ are finite. This follows from [Sp] (see [Ba, Chap. 5.1]). In paragraph 3 we will give a formula for the relation between h_{G} and h_1 in the case that the discriminant is not a square.

2. Binary quadratic forms and modules

For the following discussion it is enough that $\mathbf{K}$ is a field of characteristic $\neq 2$ and $\mathcal{O}$ an integral domain with quotient field $\mathbf{K}$. To each binary quadratic form of non–zero discriminant Δ one naturally associates a free module of rank two over $\mathcal{O}$ by factorizing the form in the extension $\mathbf{L}$ of $\mathbf{K}$ by the square root of the discriminant. $\mathbf{L}$ is separable over $\mathbf{K}$. If the discriminant is a square then $\mathbf{L}$ is isomorphic to $\mathbf{K} \times \mathbf{K}$, on which conjugation is given by exchanging the factors, if not, then $\mathbf{L}$ is isomorphic to the algebraic number field $\mathbf{K}(\sqrt{\Delta})$ with conjugation * given in the obvious way. For $x \in \mathbf{L}$ let $\mathrm{N}(x) := xx^*$ denote the relative norm of x. In the sequel we restrict to the case that Δ is not a square. Then the coefficient a of the form $\Phi(x, y) = ax^2 + bxy + cy^2$ of discriminant Δ is always non–zero and the module $M_\Phi = [a, \frac{b-\sqrt{\Delta}}{2}]_{\mathcal{O}}$ in $\mathbf{L}$ has the property that its elements fulfil

$$\frac{1}{a}\mathrm{N}(ax + \frac{b - \sqrt{\Delta}}{2}y) = \Phi(x, y). \tag{2.1}$$

This correspondence is not one to one since for example the conjugate module gives the same form. For 1–equivalence I. Kaplansky [Ka1] has introduced the notion of pairs and stated a one to one correspondence in these terms. We extended it to G–equivalence. We display it here by looking simultaneously at G– and 1–equivalence. A *pair* $[A, a]$ consists of a free module A of rank 2 over $\mathcal{O}$ in $\mathbf{L}$ and a non-zero element $a \in \mathbf{K}$. The concepts of involution, norm, product, discriminant and different are extended to pairs:

$$(2.2)\qquad [A,a]^* = [A^*,a], \quad N[A,a] = \frac{\mathrm{N}(A)}{a}, \quad [A,a][B,b] = [AB,ab].$$

If one fixes a basis x, y of A the discriminant of A with respect to that basis is

$$(2.3)\qquad \mathrm{D}(A) := (xy^* - x^*y)^2, \text{ the different } \delta(A) := (xy^* - x^*y)$$

and one sets

$$(2.4)\qquad \mathrm{D}([A,a]) := \frac{\mathrm{D}(A)}{a^2}, \quad \delta([A,a]) := \frac{\delta(A)}{a}.$$

Let $[A,a]$ be a pair of discriminant Δ. After fixing a square root δ of Δ a basis of A is called *admissible* if

$$(2.5)\qquad \delta([A,a]) = \delta.$$

An admissible basis always exists [Ka1, §5].

The essential point is that the different δ transforms in a good manner under base change by an element of G. In particular it is invariant under $\mathrm{SL}(2,\mathcal{O})$.

Suppose we are in the situation (2.1). The operation of a matrix $g = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \in G$ on (x,y) from the right corresponds on the module level to base transformation by multiplication with g from the right, namely for the basis $\{a', b'\}$ and $(x,y) := a'x + b'y$:

$$(x,y)g = (\alpha x + \gamma y, \beta x + \delta y) = (a'\alpha + b'\gamma)x + (a'\beta + b'\delta)y.$$

Given a base of a free module A of rank 2 a base transformation of determinant ϵ changes the corresponding discriminant $\mathrm{D}(A)$ and different $\delta(A)$ by the factor ϵ^2 and ϵ respectively. The pair $[A,a]$ together with an admissible basis gives the form $\Phi_A := \frac{N}{a}$, whose discriminant $\Delta(\Phi_A)$ is equal to $\mathrm{D}([A,a])$. One defines

2.1. Definition. *Two pairs $[A,a], [B,b]$ are called G–equivalent if there exists $\lambda \in \mathbf{L}^*$ and $\epsilon \in \mathcal{O}^*$ such that $\lambda A = B$ and $\epsilon \mathrm{N}(\lambda)a = b$. When $\epsilon = 1$ then they are called 1-equivalent.*

Analoguous to [Ka1, Theorem 1] this leads to

2.2. Lemma. *Let $\mathbf{K}$ be a field of char $\neq 2$, Let $\mathcal{O}$ be integral domain with quotient field $\mathbf{K}$. For a given discriminant Δ fix a square root $\delta \in \mathbf{L}$. Then a one to one correspondence of G–equivalence (resp. 1–equivalence) classes of binary quadratic forms over $\mathcal{O}$ of discriminant Δ and G–equivalence (resp. 1–equivalence) classes of pairs of discriminant Δ is given by choosing for $[A,a]$ an admissible basis and taking the norm form $\frac{N}{a}$ with respect to that basis.*

Proof. We only consider G–equivalence. We look at the map from pairs to forms. Surjectivity follows by (2.1) and by the fact that for a form Φ' which is G–equivalent to Φ under the matrix g we get the pair $\left[\left[a, \frac{b-\sqrt{\Delta}}{2}\right]_{\mathcal{O}}, \det(g)a\right]$ with:

$$\Phi' = \frac{N_g(x,y)}{\det(g)a} = \det(g)^{-1}\frac{\mathrm{N}((x,y)g)}{a} = \det(g)^{-1}\Phi((x,y)g).$$

N_g denotes the norm form with respect to the basis transformed by g. The resulting basis is admissible because the factor $\det(g)$ in the different of the transformed basis is cancelled by that of $\det(g)a$. The two pairs are G–equivalent (with $\lambda = 1$). Hence the pre–image of a G–equivalence class of forms lies in a G–equivalence class of pairs.

On the other hand one has to show that the forms that are given by two G–equivalent pairs $[A, a], [B, b]$ by taking the norm form with respect to a chosen admissible basis are G–equivalent. This we do in two steps. First: $\lambda = 1$, i.e. $A = B$ and $\epsilon a = b$ for some $\epsilon \in \mathcal{O}^*$: Let $\{x, y\}$ be admissible basis for $[A, a]$ and $\{u, v\}$ admissible basis for $[B, b]$. It suffices to show that there exists a base transformation of determinant ϵ. Since $A = B$ there exists a matrix $g \in \mathrm{G}$ such that $[u, v] = [x, y]g$. Looking at the differents for the given bases we see:

$$b\delta = \epsilon a\delta = \delta(B) = \det(g)\delta(A) = \det(g)a\delta.$$

Therefore: $\det(g) = \epsilon$. Second step: $\lambda \neq \{0, 1\}$. Is $\{x, y\}$ admissible basis for $[A, a]$ then $\{\lambda x, \lambda y\}$ is admissible basis for $[B, \mathrm{N}(\lambda)a]$ and the corresponding forms are the same. Then we apply step 1 to $[B, \mathrm{N}(\lambda)a]$ and $[B, b]$. This shows that G–equivalent pairs give G–equivalent forms.

One shows injectivity with the same arguments as in [Ka1, §5]; it is crucial that the different of the pair with respect to an admissible basis behaves well under G–equivalence. □

3. The automorphism group of a binary quadratic form

Now we return to the case that $\mathbf{K}$ is a number field. The following discription of the automorphism group $\mathrm{E}(\Phi)$ is along the lines of [Z1, §8, Satz 2]. The calculations are basically the same but for an arbitrary number field the conclusion is not as nice as over $\mathbf{Z}$ because the divisibility by 2 arguments don't work in the general case. We only give the result and remark with respect to the proof that one has to use the prime ideal factorization in $\mathcal{O}$.

3.1. Lemma. *The map*

$$\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \longmapsto (\delta + \alpha, \gamma/\alpha) \tag{3.2}$$

is a bijection from $\mathrm{E}(\Phi)$ *onto the union over all invertible* $\epsilon \in \mathcal{O}$ *of the set of solutions of* $t^2 - \Delta u^2 = 4\epsilon$ *with* $u \in (a, b, c)_{\mathcal{O}}^{-1}$ *and* $t \equiv bu \mod 2\mathcal{O}$.

The operation of $g \in \mathrm{E}(\Phi)$ on the basis of the module A associated to the binary quadratic form is like multiplication by a unit of the endomorphism ring $\mathcal{O}_A := \{l \in \mathbf{L} : lA \subset A\}$ of A:

$$\left[a, \frac{b - \sqrt{\Delta}}{2}\right]_{\mathcal{O}} g = \frac{t - \sqrt{\Delta}u}{2} \left[a, \frac{b - \sqrt{\Delta}}{2}\right]_{\mathcal{O}} = A. \tag{3.3}$$

Because of Lemma 3.1 $\frac{t-\sqrt{\Delta}u}{2}$ is a unit in $\mathcal{O}_A$. On the other hand it is shown in [Sp, §3] that a multiplication by a unit E of $\mathcal{O}_A$ can be expressed as a transformation from the right by a matrix in $\mathrm{E}(\Phi)$, its determinant is $\mathrm{N}_{L/K}(E)$ $(= \mathrm{N}(E))$. Hence

$$\mathrm{E}(\Phi) \simeq \mathcal{O}_A^* \text{ and } \mathrm{E}_1(\Phi) \simeq \{\epsilon \in \mathcal{O}_A^* | \mathrm{N}(\epsilon) = 1\}. \tag{3.4}$$

With the definitions of the previous chapter we deduce:

3.2. Lemma. *The G–equivalence class of a pair $[A, a]$ (and hence of the corresponding binary quadratic form) splits into $[\mathcal{O}^* : \mathrm{N}(\mathcal{O}_A^*)] < \infty$ 1–equivalence classes.*

Proof. Assume $[A, a]$ and $[B, b]$ are G–equivalent, this is $B = \lambda A$ and $b = \mathrm{N}(\lambda)\epsilon a$ for some $\lambda \in \mathbf{L}^*$ and $\epsilon \in \mathcal{O}^*$. Then A and B have the same endomorphism ring $\mathcal{O}_A$. Multiplication by a unit ϵ_A of $\mathcal{O}_A$ leaves A and B invariant. Hence $[A, a]$ is also G–equivalent to $[B, \mathrm{N}(\epsilon_A)b]$. If the above ϵ is equal to $\mathrm{N}(\epsilon_A)$ for some $\epsilon_A \in \mathcal{O}_A^*$ then $[B, \mathrm{N}(\epsilon_A^{-1})b]$ is 1–equivalent to $[A, a]$ for $\lambda' := \epsilon_A^{-1}\lambda$. Otherwise $[A, a]$ and $[B, b]$ are not 1–equivalent. $[\mathcal{O}^* : \mathrm{N}(\mathcal{O}_A^*)]$ is finite since $\{\epsilon^2 | \epsilon \in \mathcal{O}^*\}$ is contained in $\mathrm{N}(\mathcal{O}_A^*)$ which has finite index in $\mathcal{O}^*$. This shows the assertion. □

4. The endomorphism ring of a free module of rank 2

About endomorphism rings of full modules in a field see also [B–Sh]. We always suppose that $\Delta \in \mathcal{O}$ is not a square; $A = \left[a, \frac{b-\sqrt{\Delta}}{2}\right]_{\mathcal{O}}$ is the module associated to the form $\Phi(x, y) = ax^2 + bxy + cy^2$ of discriminant Δ, $\mathfrak{Q} := (a, b, c)_{\mathcal{O}}^{-1}$ and $\mathbf{L} = \mathbf{K}(\sqrt{\Delta})$. In this paragraph we study the relation between the endomorphism ring $\mathcal{O}_A = \{l \in \mathbf{L} : lA \subset A\}$ of A, $\mathcal{O}$ and the integral closure of $\mathcal{O}$ in $\mathbf{L}$, in particular one will see that if the $\mathcal{O}_A$ is free over $\mathcal{O}$ then the finitely generated, free, proper ideals of $\mathcal{O}_A$ form a subgroup of the group of regular ideals of $\mathcal{O}_A$. The structure of $\mathcal{O}_A$ is as follows:

4.1. Lemma. *$\mathcal{O}_A$ is an order in $\mathcal{O}_{\mathbf{L}}$ and* $\mathcal{O}_A = \mathcal{O} \oplus \frac{b-\sqrt{\Delta}}{2}\mathfrak{Q}$.

Proof. It follows from the definition that $\mathcal{O}_A$ is a ring with 1. It is a subring of $\mathcal{O}_{\mathbf{L}}$ since it preserves a lattice.

Obviously $\mathcal{O}_A = \mathcal{O}_{yA}$ for all $0 \neq y \in \mathbf{L}$. For convenience we calculate in $\frac{1}{a}A$. Each element of $\mathbf{L}$ can be written uniquely as a $\mathbf{K}$-linear combination of 1 and $\frac{b-\sqrt{\Delta}}{2a}$. $\frac{b-\sqrt{\Delta}}{2}$ is integral since it solves $z^2 - bz + ac = 0$; therefore $\frac{b-\sqrt{\Delta}}{2a}$ solves

$$az^2 - bz + c = 0. \tag{4.1}$$

We see

$$l = x + y\frac{b-\sqrt{\Delta}}{2a} \quad \in \mathcal{O}_A, \quad x, y \in \mathbf{K},$$

$$\Longleftrightarrow l \in A \quad \text{and} \quad l\frac{b-\sqrt{\Delta}}{2a} \quad \in A$$

$$\Longleftrightarrow x + y\frac{b-\sqrt{\Delta}}{2a} \in A \quad \text{and}$$

$$x\frac{b-\sqrt{\Delta}}{2a} + y\left(\frac{b-\sqrt{\Delta}}{2a}\right)^2 = x\frac{b-\sqrt{\Delta}}{2a} + y\frac{b}{a}\frac{b-\sqrt{\Delta}}{2a} - y\frac{c}{a} \quad \in A \quad \text{by (4.1)}$$

$$\Longleftrightarrow x, y, y\frac{b}{a}, y\frac{c}{a} \in \mathcal{O}.$$

By the prime ideal factorization of the principal ideal generated by a coefficient of Φ one checks that the condition on y is equivalent to

$$y \in (a)\mathfrak{Q}.$$

Hence $\mathcal{O}_A = \mathcal{O} + \frac{b-\sqrt{\Delta}}{2a}(a)\mathfrak{Q} = \mathcal{O} + \frac{b-\sqrt{\Delta}}{2}\mathfrak{Q}$. $\mathcal{O}_A\mathbf{K} = \mathbf{L}$. Hence $\mathcal{O}_A$ is an order. □

4.2. Corollary. *$\mathcal{O}_A$ is a free module over $\mathcal{O}$ if and only if $(a,b,c)_\mathcal{O}$ is a principal ideal.*

4.3. Definition. *We call $\Phi(x,y) = ax^2 + bxy + cy^2$ 'primitive' if $(a,b,c)_\mathcal{O} = \mathcal{O}$, and 'semi-primitive' if $(a,b,c)_\mathcal{O}$ is a principal ideal.*

4.4. Remark: i) Since $A \subset \mathbf{L}$ is finitely generated over $\mathcal{O}$ there exists $l \in \mathbf{L}^*$ such that $l \cdot A \subset \mathcal{O}_A$, $l \cdot A$ is an ideal of $\mathcal{O}_A$. We call A and B similar if there exists $l \in \mathbf{L}$ such that $l \cdot A = B$.

ii) When $\mathcal{O}_A$ is free one can determine its discriminant $\mathrm{D}(\mathcal{O}_A)$ (see (2.3)). Let $B = [a_1 + a_2 d, b_1 + b_2 d]_\mathcal{O}$ be an ideal of $\mathcal{O}_A = [1, d]_\mathcal{O}$. Their discriminants fulfil the identity $\mathrm{D}(B) = (a_1 b_2 - a_2 b_1)^2 \mathrm{D}(\mathcal{O}_A)$.

iii) If $\mathcal{O}$ is a principal ideal domain then every ideal of $\mathcal{O}_A$ is free over $\mathcal{O}$.

To study the relation between $\mathcal{O}_A$ and $\mathcal{O}_\mathbf{L}$ we first look at a more general situation. Let $R \subset R'$ be commutative rings, $\mathfrak{f} := Ann(R'/R) := \{l \in R' : lR' \subset R\}$ the conductor of R in R'. We say

4.5. Definition. *i) A R–module A 'belongs to' or 'is proper for' R if $\mathcal{O}_A = R$.*

ii) A R–ideal $A \subset$ Quot(R) is called '1–regular' if $(A,\mathfrak{f})_R = R$, an R'–ideal $A \subset Quot(R')$ '1–regular' if $(A,\mathfrak{f})_{R'} = R'$. Here $(A,\mathfrak{f})_R$ denotes the R–module generated by the elements of A and $\mathfrak{f}$.

iii) A R–ideal $A \subset Quot(R)$ is called 'regular' if it is similar to a 1–regular ideal, i.e. there exists $l \in Quot(R)$ such that $l \cdot A \subset R$ and $(l \cdot A, \mathfrak{f})_R = R$, a R'–ideal $A \subset Quot(R')$ 'regular' if, if it is similar to a 1–regular ideal, i.e. there exists $l \in Quot(R')$ such that $l \cdot A \subset R'$ and $(l \cdot A, \mathfrak{f})_{R'} = R'$.

Here 1–regularity is what is usually called regularity.

4.6. Proposition. *Let $\mathcal{O}$ be the ring of integers of an algebraic number field $\mathbf{K}$, $\mathbf{L}$ be a quadratic extension field over $\mathbf{K}$, R' the integral closure of $\mathcal{O}$ in $\mathbf{L}$. Let $A \subset \mathbf{L}$ be a finitely generated, full $\mathcal{O}$–module, i.e. it contains a $\mathbf{K}$–basis of $\mathbf{L}$. Then*

i) A is invertible in its endomorphism ring $R := \mathrm{End}(A) := \{x \in \mathbf{L} \mid xA \subset A\}$, i.e. there exists a module $\hat{A}$ belonging to R such that $A\hat{A} = R$, namely $\hat{A} = \{x \in \mathbf{L} : xA \subset R\}$.

ii) R is noetherian as $\mathcal{O}$–module, $\mathcal{O} \subset R$.

iii) The finitely generated proper ideals for R are exactly the finitely generated R–regular ideals.

To proof the proposition we need to prove some lemmata first. The same conditons as in the proposition are imposed.

Lemma 4.7. *A is invertible in R if and only if $A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$ is invertible in $R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$ for each prime ideal $\mathfrak{p}$ of $\mathcal{O}$. $\mathcal{O}_{\mathfrak{p}}$ denotes the localization of $\mathcal{O}$ at $\mathfrak{p}$.*

Proof. $\mathcal{O}_{\mathfrak{p}}$ is a flat $\mathcal{O}$–module. Therefore the map $A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}} \mapsto R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$ is injective. Furthermore by the definition of localization $A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}} = \{\frac{a}{s} \mid a \in A,\ s \in \mathcal{O} \setminus \mathfrak{p}\}$, the same for R, and $(AB) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}} = (A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}})(B \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}})$ for A and B both satisfying the conditions of Proposition 4.6.

$R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$ is equal to the endomorphism ring $\mathrm{End}(A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}})$ of $A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$. $R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}} \subset \mathrm{End}(A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}})$ is clear. To show $\mathrm{End}(A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}) \subset R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$ we choose a set of generators $\{a_1, \ldots, a_n\}$ of A over $\mathcal{O}$. For $x \in \mathrm{End}(A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}})$

$$xa_i = \frac{b_i}{y_i} \quad \text{for } b_i \in A, \quad y_i \in \mathcal{O} \setminus \mathfrak{p}.$$

The element $z := y_1 \times \cdots \times y_n x$ is in R and hence $x = \frac{z}{y_1 \times \cdots \times y_n} \in R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$.

If A is invertible with inverse module B, i.e. $AB = R$, then $(AB) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}} = (A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}})(B \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}) = R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$ for each prime ideal $\mathfrak{p} \in \mathcal{O}$ and therefore $A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$ is invertible with invers module $B \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$.

Now suppose that $A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$ is invertible for each prime ideal $\mathfrak{p} \in \mathcal{O}$ and denote the invers module by $B_{\mathfrak{p}}$. By [Bou, Chap.II, Par. 3, Cor. 4] $A = \bigcap_{\mathfrak{p} \in \mathcal{O}} A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$. Furthermore $AB = \bigcap_{\mathfrak{p} \in \mathcal{O}} (A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}) \bigcap_{\mathfrak{p} \in \mathcal{O}} (B \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}) = \bigcap_{\mathfrak{p} \in \mathcal{O}} (AB) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$. Set $B := \bigcap_{\mathfrak{p} \in \mathcal{O}} B_{\mathfrak{p}}$. We see

$$AB = \bigcap_{\mathfrak{p} \in \mathcal{O}} (A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}) B_{\mathfrak{p}} = \bigcap_{\mathfrak{p} \in \mathcal{O}} R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}} = R.$$

B fulfils the required conditions. Hence A is invertible in R with inverse module B. □

Lemma 4.8. *$A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$ is invertible in $R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$.*

Proof. Since A is a torsionfree full $\mathcal{O}$–module in $\mathbf{L}$ and $\mathbf{L}$ is a quadratic extension of $\mathbf{K}$ the module A is projective of rank two over $\mathcal{O}$ and $A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$ is free of rank two over $\mathcal{O}_{\mathfrak{p}}$ ($\mathcal{O}$ is Dedekind!). We denote the involution on $\mathbf{L}$ which only fixes $\mathbf{K}$ by *. We will construct the inverse module using this involution.

First we show $R^* = R$. R is contained in O_L since it stabilizes a lattice in L, namely A viewed as a free $\mathbf{Z}$–module. It contains $\mathcal{O}$ by definition. Hence $\mathrm{tr}(r) = r + r^* \in \mathcal{O}$ and

$\mathrm{tr}(r) - r = r^* \in R$. Therefore $R^* \subset R$. Furthermore $(R^*)^* = R$, hence $R \subset R^*$ and the assertion follows.

It follows that the endomorphism ring of $(A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}})^*$ is $R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$ since $(R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}})^* = R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$ for each $\mathfrak{p} \in \mathcal{O}$. The product $(A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}})(A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}})^*$ is invariant under * and therefore generated by elements in $\mathcal{O}_{\mathfrak{p}}$ (An irreducible divisor of the different of $R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$, i.e. the ideal of R generated by $r - r^*$, $r \in R$, will appear to an even power). Since $\mathcal{O}_{\mathfrak{p}}$ is a principal ideal domain one has

$$(A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}})(A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}})^* = N_A(R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}})$$

with $0 \neq N_A \in \mathcal{O}_{\mathfrak{p}}$ and we can take $N_A^{-1}(A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}})^* =: A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}^{-1}$ as inverse module to A. □

Proof of Proposition 4.6: i): By commutativity the inverse is unique for if $AB = AB' = R$ then $B = BR = BAB' = RB' = B'$. By Lemma 4.7 and 4.8 $A^{-1} = \bigcap_{\mathfrak{p} \in \mathcal{O}} N_A^{-1}(A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}})^*$. Now we show $A^{-1} = \hat{A}$. $A^{-1} \subset \hat{A}$ holds by the definition of $\hat{A}$. Since $A\hat{A} \subset R = A^{-1}A$ we see by multiplication with A^{-1} that $\hat{A} \subset A^{-1}$.

ii): A is an $\mathcal{O}$–module. Therefore by definition R is an $\mathcal{O}$–module and $\mathcal{O} \subset R$. $\mathcal{O}$ is noetherian. R is finitely generated since (stabilizing a lattice, namely A over $\mathbf{Z}$) it is contained in $\mathcal{O}_{\mathbf{L}}$ which is a noetherian $\mathcal{O}$–module. Hence R itself is noetherian as $\mathcal{O}$–module.

iii): If A is R–regular then it is R–proper. For if $A \subset R$ is not R–proper then $R \subsetneq \mathrm{End}(A) =: R' \subset \mathcal{O}_{\mathbf{L}}$. Set $\mathfrak{f}' := \mathrm{Ann}(R'/R)$. $\mathfrak{f}'$ is the largest ideal of R' contained in R, $\mathfrak{f}' \neq R$. Hence $A \subset \mathfrak{f}'$. On the other hand $\mathfrak{f} := \mathrm{Ann}(\mathcal{O}_{\mathbf{L}}/R)$ is contained in $\mathfrak{f}'$ since $R'\mathfrak{f} \subset R$, hence $\mathfrak{f} \subset \mathfrak{f}'$ and $(A, \mathfrak{f}') \subset \mathfrak{f}' \neq R$, i.e. A is not R–regular.

We show that a proper R–ideal A is regular by proving that it is locally principal, i.e. $A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}} = a_{\mathfrak{p}}(R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}})$ for some $a_{\mathfrak{p}} \in R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$ for each prime ideal $\mathfrak{p} \subset \mathcal{O}$. Obviously a principal ideal is regular. By the same argument as for [Oh, Prop. 2] one shows that A is R–regular if and only if $A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$ is $R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$–regular for all $\mathfrak{p} \subset \mathcal{O}$.

Now we show that A is locally principal. Since $A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$ is invertible we can conclude by [Ka2, Thm 2] that

$$A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}} = a_{\mathfrak{p}} S_{\mathfrak{p}}$$

where $S_{\mathfrak{p}}$ is an order, i.e. a finitely generated $\mathcal{O}_{\mathfrak{p}}$–module which is a subring of $\mathbf{L}$ containing 1 such that $S_{\mathfrak{p}}\mathbf{K} = \mathbf{L}$, and $a_{\mathfrak{p}} \in \mathbf{L}$ invertible. $S_{\mathfrak{p}} \subset R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$ since $S_{\mathfrak{p}}(A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}) = S_{\mathfrak{p}} a_{\mathfrak{p}} S_{\mathfrak{p}} = a_{\mathfrak{p}} S_{\mathfrak{p}} = A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$. On the other hand $(R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}) a_{\mathfrak{p}} S_{\mathfrak{p}} = (R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}})(A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}) \subset (A \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}) = a_{\mathfrak{p}} S_{\mathfrak{p}}$. Multiplying by $a_{\mathfrak{p}}^{-1}$ we get $(R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}) S_{\mathfrak{p}} \subset S_{\mathfrak{p}}$ and since $1 \in S_{\mathfrak{p}}$ we see $(R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}) \subset S_{\mathfrak{p}}$. Hence

$$S_{\mathfrak{p}} = R \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}.$$

This shows iii). □

Corollary 4.9. *The finitely generated, proper R–modules form a group under module multiplication (we denote it by $\mathfrak{R}$). The proper ideals of R are finitely generated.*

4.10. Remark: i) It also follows from [Ka2, §2] that the relative norm defined by the involution is multiplicative.

ii) The correspondence between 1–regular R–ideals and 1–regular R'–ideals is one to one and for a 1–regular R–ideal A the index satisfies

$$[R : A] = [R' : AR'], \tag{4.2}$$

(see for example [Co, Thm. 10.19]). There are only finitely many similarity classes of finitely generated, proper R–modules (cf. Remark 4.4 and [B–Sh]), by Corollary 4.9 they form a group which we denote by $C(\mathfrak{N})$. Each similarity class can be represented by a 1–regular ideal. The 1–regular ideals have a unique prime ideal factorization in R.

We used in the proof of Proposition 4.6 that each finitely generated, torsionfree module A over a Dedekind ring $\mathcal{O}$ is projective and by this isomorphic to a direct sum of $n := rk_{\mathcal{O}} A$ ideals of $\mathcal{O}$ and

$$A \cong \mathfrak{P}_1 \oplus \ldots \oplus \mathfrak{P}_n \cong \mathcal{O} \oplus \ldots \oplus \mathcal{O} \oplus \mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_n, \tag{4.3}$$

$\mathcal{O}$ taken $n-1$–times (see J. Milnor [Mi, §1]). Using the property of regularity one can generalize the proof of (4.3) given in [Mi, Lemma 1.7] to direct sums of *proper* R–modules:

4.11. Proposition. *If A and B are finitely generated proper R–modules then $A \oplus B \cong R \oplus AB$.*

Proof. One only needs to apply an additional isomorphism, namely the multiplication of A and B by the factor λ_A, λ_B resp., such that $\lambda_A A$, $\lambda_B B$ resp., are 1–regular. The 1–1–correspondence mentioned in 4.10 ii) allows one to use the same further arguments.

For the rest of this paragraph $\mathcal{O}$ and R are like in Proposition 4.6. An important consequence of the above structure theory are the following lemma and its corollary:

4.11. Lemma. *Let $\mathcal{I}$ be the ideal class group of $\mathcal{O}$ and $[\mathfrak{P}]$ denote the class of the $\mathcal{O}$–ideal $\mathfrak{P}$ in $\mathcal{I}$; $\mathfrak{N}$ the group of finitely generated R–proper R–modules. The map*

$$\begin{aligned} \varphi : \mathfrak{N} &\longrightarrow \mathcal{I} \\ A &\longmapsto [\mathfrak{P}_A], \end{aligned} \tag{4.4}$$

$(A \cong \mathcal{O} \oplus \mathfrak{P}_A)$, is a homomorphism if and only if R is free over $\mathcal{O}$.

Proof. For two modules $A, B \in \mathfrak{N}$ we have to show $\varphi(AB) = \varphi(A)\varphi(B)$. According to Proposition 4.11 $A \oplus B \cong R \oplus AB$. Now we apply (4.3) to A, B, AB and R. Assume $R \cong \mathcal{O} \oplus \mathfrak{P}_R$, we get the following diagram of isomorhpisms:

$$\begin{array}{ccccc} A \oplus B & \cong_{\mathcal{O}} & \mathcal{O} \oplus \mathfrak{P}_A \oplus \mathcal{O} \oplus \mathfrak{P}_B & \cong_{\mathcal{O}} & \mathcal{O} \oplus \mathcal{O} \oplus \mathcal{O} \oplus \mathfrak{P}_A \mathfrak{P}_B \\ \| \wr_R & & & & \\ R \oplus AB & \cong_{\mathcal{O}} & \mathcal{O} \oplus \mathfrak{P}_R \oplus \mathcal{O} \oplus \mathfrak{P}_{AB} & \cong_{\mathcal{O}} & \mathcal{O} \oplus \mathcal{O} \oplus \mathcal{O} \oplus \mathfrak{P}_R \mathfrak{P}_{AB} \end{array}$$

Hence $\mathfrak{P}_R \mathfrak{P}_{AB} \cong_{\mathcal{O}} \mathfrak{P}_A \mathfrak{P}_B$. Such an isomorphism is a multiplication by a constant in $\mathbf{K}^*$ [Mi, Thm. 1.6] therefore $[\mathfrak{P}_R \mathfrak{P}_{AB}] = [\mathfrak{P}_A \mathfrak{P}_B]$. $\varphi(AB) = [\mathfrak{P}_{AB}] = [\mathfrak{P}_A \mathfrak{P}_B] = \varphi(A)\varphi(B)$ if and only if $\mathfrak{P}_R$ is a principal ideal, i.e. R is free over $\mathcal{O}$. $\square$

4.13. Corollary. *If R is free over $\mathcal{O}$ then regular and also the 1-regular R–modules which are free over $\mathcal{O}$ form a subgroup $\mathfrak{H}$, $\mathfrak{H}_1$ resp., of $\mathfrak{R}$.*

Proof. The 1-regular R–modules form a subgroup $\mathfrak{R}_1$ of $\mathfrak{R}$. $\mathfrak{H}$ is the kernel of φ, $\mathfrak{H}_1$ the kernel of the restriction of φ to $\mathfrak{R}_1$. □

In the following we will use two other important facts:

4.14. Lemma. *Let R be an order in* **L**, *that is free over $\mathcal{O}$, A be a regular R–ideal, free over $\mathcal{O}$ (i.e. $A \in \mathfrak{H}$). Then its norm ideal $N(A) = AA^*$ is principal.*

Proof. Choose an admissible basis (see (2.5)) $\{a, b\}$ of the pair $[A, 1]$ over $\mathcal{O}$. The norm form of this pair gives the binary quadratic form $\Phi_A = aa^*x^2 + 2\Re(ab^*)xy + bb^*y^2$ of the discriminant $\Delta = 4\Re(ab^*)^2 - 4aa^*bb^*$. This form leads to the 'standard pair' $A' = [[aa^*, \frac{2\Re(ab^*)-\sqrt{\Delta}}{2}], aa^*]$ which is according to Lemma 2.2 G–equivalent to $[A, 1]$. Therefore A' is also a regular R–module. Since R is assumed to be free by Corollary 4.2 Φ is semi-primitive, i.e. the ideal generated by the coefficients of Φ is principal:

$$(aa^*, 2\Re(ab^*), bb^*)_{\mathcal{O}} =: (r)_{\mathcal{O}} \tag{4.5}$$

for some $0 \neq r \in \mathcal{O}$. On the basis of the 'standard pair' one checks that $A'(A')^* = aa^*rR$. But this is the norm ideal. □

4.15. Fact: A free order R of rank 2 over $\mathcal{O}$ is uniquely determined by its discriminant.

5. On zeta functions of primitive binary quadratic forms

Let $\mathcal{O}$ be the ring of integers of an algebraic number field K. Fix $\Delta \neq 0$ in $\mathcal{O}$ which is not a square. The binary quadratic forms over $\mathcal{O}$ of discriminant Δ factorize in the relative quadratic field extension **L** of **K** by $\sqrt{\Delta}$. For a primitive form the free module of the corresponding pair is similar (see Remark 4.4 i) to a proper ideal of the unique order R of discriminant Δ which is free over $\mathcal{O}$ (see (2.4) and Lemma 4.1). The finitely generated, free, proper modules of R form a subgroup $\mathfrak{H}$ of the group of finitely generated, proper modules $\mathfrak{R}$ and hence the similarity classes of the free proper modules, denoted by $C(\mathfrak{H})$, form a subgroup of the finite class group $C(\mathfrak{R})$ of proper modules of R (see Remark 4.10 and Corollary 4.13). From this and Lemma 4.14 follows that the correspondence between primitive binary quadratic forms over $\mathcal{O}$ and pairs:

5.1. Lemma. *For above $\Delta \in \mathcal{O}$ fix a square root $\delta \in$* **L**. *Then there is a one to one correspondence between G–equivalence classes of primitive binary quadratic forms over $\mathcal{O}$ of discriminant Δ and similarity classes of finitely generated, free (over $\mathcal{O}$), proper R–modules by choosing an admissible basis of a representing module $A \subset R$ for the form with respect to a generator $n(A)$ of the norm ideal $\mathrm{N}(A) = AA^*$ and taking the norm form $\frac{N}{n(A)}$ with respect to that basis.*

Proof. For each similarity class of finitely generated, free proper modules choose a representative A which is an ideal. One naturally can associate to it the G–equivalence class of the pair (see Def. 2.1) $[A, n(A)]$, where n(A) is a generator of the principal ideal $\mathrm{N}(A)$ (see Remark 4.10 i and Lemma 4.14). It follows from Remark 4.4 ii) and Lemma 4.1 that the discriminant $\mathrm{D}(A)$ of A (for the admissible basis) is equal to $n(A)\Delta$, hence the pair has discriminant Δ. The only other pairs of discriminant Δ for some basis of A are $[A, \epsilon n(A)]$, $\epsilon \in \mathcal{O}^*$, but these are G–equivalent to $[A, n(A)]$. On the other hand by primitivity of the form $\Phi(x,y) = ax^2 + bxy + cy^2$ and Corollary 4.2 the associated module $[a, \frac{b-\sqrt{\Delta}}{2}]_{\mathcal{O}}$ is proper for R $(= [1, \frac{b-\sqrt{\Delta}}{2}]_{\mathcal{O}})$. □

Lemma 5.1 and Corollary 4.13 motivate the following definitions of zeta functions. We will show that they are equal. In the definition we do not specify the region of convergence because it will follow from Lemma 5.4 and Proposition 5.9 that the functions considered can be meromorphically continued to **C**. We only remark that if they converge for large s then they converge absolutely. So we are allowed to change the summation.

5.2. Definition. *For the unique free order R of rank 2 over $\mathcal{O}$ of discriminant Δ set*

$$Q_\Delta(s) := \sum_{\substack{A \subset R, \text{ proper ideal} \\ \text{free over } \mathcal{O}}} \mathrm{N}_R(A)^{-s}.$$

Furthermore, let $[\Phi]$ denote the G–equivalence class of the binary quadratic form Φ over $\mathcal{O}$, $\mathrm{E}(\Phi)$ the automorphism group of Φ. Set

$$P_\Delta(s) := \sum_{\substack{[\Phi] \\ \Phi \text{ primitive} \\ \Delta(\Phi)=\Delta}} \sum_{(x,y)\in(\mathcal{O}\times\mathcal{O})/\mathrm{E}(\Phi)} |\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\Phi(x,y))|^{-s}.$$

where

$$\mathrm{N}_R(A) := \mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\mathrm{N}(A)). \tag{5.1}$$

5.3. Lemma. $P_\Delta(s) = Q_\Delta(s)$.

Proof. We start with $Q_\Delta(s)$. Let $\{H_1, \ldots, H_r\}$ denote the similarity classes of $\mathfrak{H}$. Then

$$Q_\Delta(s) = \sum_{i=1}^{r} Q_{\Delta,i}(s),$$

with $Q_{\Delta,i}(s) := \sum_{A\in H_i} \mathrm{N}_R(A)^{-s}$. For a proper ideal $A \subset R$ one has a one–to–one correspondence between principal ideals $(\xi)_R$, $\xi \in A$, and proper ideals B in the similarity class of A^{-1} by construction of the inverse module (see Proposition 4.6):

$$AB = (\xi)_R \Longleftrightarrow B = (\xi)_R A^{-1}, \qquad B \subset R \text{ if and only if } (\xi)_R \subset (A^{-1})^{-1} = A. \tag{5.2}$$

Take for each class H_i a representative ideal A_i. Then by (5.1), (5.2) and the fact that A^{-1} is similar to A^* (consequence of Lemma 4.14, i.e. $A^{-1} = \mathrm{N}(A)^{-1}A^*$ with $\mathrm{N}(A)$ principal) it follows:

$$Q_{\Delta,i}(s) = \sum_{\xi\in A_i/U_R} \mathrm{N}_{\mathbf{K}/\mathbf{Q}}\left(\frac{\mathrm{N}(\xi)}{\mathrm{N}(A_i)}\right)^{-s},$$

where U_R denotes the units of R. By the choice of a generator $n(A)$ of $\mathrm{N}(A)$ and an admissible basis with respect to this generator we get a binary quadratic form Φ_i of discriminant Δ. Dividing out the units U_R is by Remark 3.1 equivalent to dividing out the action of the automorphism group $\mathrm{E}(\Phi_i)$ with respect to the above basis, hence

$$Q_{\Delta,i}(s) = \sum_{(x,y)\in(\mathcal{O}\times\mathcal{O})/\mathrm{E}(\Phi_i)} |\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\Phi_i(x,y))|^{-s}.$$

The absolute value has to be taken since $\mathrm{N}_{\mathbf{K}/\mathbf{Q}}((a)) = |\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(a)|$. By Lemma 5.1 (1–1 correspondence) it follows

$$P_\Delta(s) = Q_\Delta(s).$$

□

For semi–primitive forms $\Phi(x,y) = ax^2 + bxy + cy^2$ of discriminant Δ, i.e. $(a,b,c)_\mathcal{O} = (r)_\mathcal{O}$ for some $0 \neq r \in \mathcal{O}$, the endomorphism ring of the corresponding free module A has discriminant $\frac{\Delta}{r^2}$. $\frac{1}{r}\Phi(x,y)$ is primitive of discriminant $\frac{\Delta}{r^2}$. Summing over all principal square divisors of Δ one obtains a corollary of Lemma 5.3 for semi–primitive forms:

5.4. Definition and Corollary.

$$\begin{aligned} S_\Delta(s) :&= \sum_{\substack{[\Phi] \\ \Phi \text{ semi-primitive} \\ \Delta(\Phi)=\Delta}} \sum_{(x,y)\in(\mathcal{O}\times\mathcal{O})/\mathrm{E}(\Phi)} |\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\Phi(x,y))|^{-s} = \\ &= \sum_{(r)^2|\Delta} |\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(r)|^{-s} P_{\frac{\Delta}{r^2}}(s). \end{aligned}$$

Before we move on to the question of convergence we present the following, more general zeta function for primitive binary quadratic forms over $\mathcal{O}$.

5.5. Definition. *Let $M \in \mathcal{O}$ be an ideal. Define the following zeta function (compare: Definition 5.2) :*

$$P_{M,\Delta}(s) := \sum_{\substack{[\Phi] \\ \Phi \text{ primitive} \\ \Delta(\Phi)=\Delta}} \sum_{(x,y)\in(M\times M)/\mathrm{E}(\Phi)} |\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\Phi(x,y))|^{-s}.$$

If A is a proper ideal in R, free over $\mathcal{O}$, then also MA is proper in R but not free except in the case that M^2 is principal (cf. (4.3)); it lies in a coset of $\mathfrak{R}$ modulo $\mathfrak{H}$. With the same arguments as in Lemma 5.3 one shows:

5.6. Lemma. *Let $\{A_i\}_{i=1,\dots,h}$ be a representative system of $C(\mathfrak{H})$. Then*

$$P_{M,\Delta}(s) = \sum_{i=1}^{h} \sum_{\substack{B\in[MA_i]^{-1} \\ \text{ideal}}} \mathrm{N}_{\mathbf{K}/\mathbf{Q}}(M)^{-2s}\mathrm{N}_R(B)^{-s}.$$

5.7. Remark: i) Here in general $(MA)^{-1}$ is not similar to $(MA)^*$ because MM^* may not be principal (compare Lemma 4.14).

ii) If the index of the group of units $U_{\mathcal{O}}$ of $\mathcal{O}$ in the group of units U_R in R is finite one can apply [EGM, Proposition 3.4] to obtain a formula in terms of $P_{M,\Delta}(s)$ for the zeta function

$$\widehat{P}_{M,\Delta}(s) := \sum_{\substack{[\Phi] \\ \Phi \text{ primitive} \\ \Delta(\Phi)=\Delta}} \sum_{\substack{(x,y)\in(M\times M)/\mathrm{E}(\Phi) \\ (x,y)=M}} |\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\Phi(x,y))|^{-s},$$

namely

$$\widehat{P}_{M,\Delta}(s) = \frac{|U_R|}{|U_{\mathcal{O}}|} \sum_{[M']\in\mathcal{I}} \zeta(M,M',s) P_{M',\Delta}(s),$$

where $[M']$ runs through the ideal classes of $\mathcal{O}$.

iii) The problem of units also leads to the fact that one can define zeta functions of binary quadratic forms with respect to 1–equivalence (see Definition 5.1) only if $\mathcal{O}$ has only finitely many units since the action of the automorphism group of the form corresponds to multiplication of the module by units of R of relative norm 1. Otherwise the inner sum does not converge. That means that $\mathbf{K}$ has to be either rational or imaginary quadratic. The G–equivalence class of a form as well as the similarity class of the the corresponding module splits into finitely many 1–equivalence classes and 1–similarity classes respectively. Two modules are 1–similar if they are similar and the relative norm of the similarity factor fulfills a restriction given by 1–equivalence of pairs (Definition 2.1).

iv) If the forms are not primitive one can formulate the zeta function only in terms of the corresponding modules, but not in terms of the order. For the zeta function of a module see [Od].

6. Analytic Continuation

The meromorphic continuation of $P_\Delta(s)$ to the whole complex plane is provided by expressing $Q_\Delta(s)$ in terms of L–functions associated to a congruence subgroup for $\mathbf{L}$. We define a zeta function $\zeta_R(s)$ for the order R in $\mathbf{L}$. Since R is noetherian each proper ideal A can be uniquely written as a product of primary ideals $A = P_1 \cdots P_r$ such that $(P_i, P_j)_R = R$ for $i \neq j$ [v.d.W, Kapitel 15, 17]. If $\mathcal{F}$ denotes the set of primary ideals of the conductor $\mathfrak{f}$ of R then either $(P_i, F)_R = R$ for all $F \in \mathcal{F}$ (and hence 1–regular) or there is a $F \in \mathcal{F}$ and $n \in \mathbf{N}$ such that $P_F^n \subset P_i, F \subset P_F$ for the prime ideal P_F associated to F (let us call these 'of Type II'). In our situation there are only finitely many primary ideals for a given prime ideal P_F and $n \in \mathbf{N}$ which satisfies the above inclusions. The product over the Type II primary ideals in the above factorization is a proper ideal of R. We call it a proper ideal of Type II. It follows that one can split the zeta function into two factors, a sum over the 1–regular ideals and a sum over the proper ideals of Type II :

$$\zeta_R(s) := \sum_{A\subset R,\text{ proper}} \mathrm{N}_R(A)^{-s} = \zeta_R(s,\mathfrak{f}) F_R(s,\mathfrak{f}),$$

with

$$\zeta_R(s,\mathfrak{f}) := \sum_{A\ 1\text{-regular}} \mathrm{N}_R(A)^{-s} \quad \text{and} \qquad F_R(s,\mathfrak{f}) := \sum_{B \text{ proper of Type II}} \mathrm{N}_R(B)^{-s}$$

where $\mathrm{N}_R(A) = \mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\mathrm{N}(A))$ (cf. (5.1)).

The same way one defines $\zeta_{R,\chi}(s,\mathfrak{f})$ for characters χ of $C(\mathfrak{R})$.

Furthermore we can define for R the zeta function

$$Z_R(s) := \sum_{A \subset R,\ \text{proper}} [R:A]^{-s}$$

and $Z_{R,\chi}(s,\mathfrak{f})$.

There is the 1–1 correspondence between 1–regular ideals in R and $\mathcal{O}_L$ respectively realized going down by intersection with R, going up by multiplication by $\mathcal{O}_L$. The corresponding absolute norms are equal: $[R:A] = [\mathcal{O}_L : A\mathcal{O}_L]$ (recall Remark 4.10 ii). Furthermore $AA^* \cap \mathcal{O} = (A\mathcal{O}_L)(A\mathcal{O}_L)^* \cap \mathcal{O}$. By [Co, Cor. 16.4] $\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\mathrm{N}(A)) = [\mathcal{O}_L : A\mathcal{O}_L]$. Therefore one can identify $\zeta_{R,\chi}(s,\mathfrak{f})$, $Z_{R,\chi}(s,\mathfrak{f})$ and $\zeta_{\mathcal{O}_L,\chi}(s,\mathfrak{f})$.

Furthermore $C(\mathfrak{R}) \simeq R(\mathfrak{f})/P_R(\mathfrak{f})$, where $R(\mathfrak{f})$ denotes the 1–regular ideals of R and

$$P_R(\mathfrak{f}) = \{\lambda = \frac{\beta}{\gamma} \in \mathbf{L} \mid \beta,\ \gamma \in \mathcal{O}_\mathbf{L},\ (\beta,\mathfrak{f}) = 1,\ (\gamma,\mathfrak{f}) = 1\}.$$

This is isomorphic to $\mathcal{O}_L(\mathfrak{f})/P(\mathfrak{f})$. $P(\mathfrak{f})$ is the ray modulo $\mathfrak{f}$, i.e. the principal ideals that are multiplicatively congruent to 1 modulo $\mathfrak{f}$ (for the definition see [Hal, §5, Def. 50]). Hence χ is a ideal character $\mod \mathfrak{f}$ and $\zeta_{\mathcal{O}_L,\chi}(s,\mathfrak{f}) = L(s,\chi)$, the L–series of L for the ideal character $\chi \mod \mathfrak{f}$ (cf. [Hal, §7, Def. 69,71]). We denote the order of $C(\mathfrak{R})$ by $h_\mathfrak{f}$. With this we recover $Q_\Delta(s)$ (see Definition 5.2) again by applying [EGM, Lemma 3.6] and we obtain:

6.1. Proposition.

$$P_\Delta(s) = Q_\Delta(s) = \frac{1}{h_\mathfrak{f}} \sum_\chi L(s,\chi) F_{R,\chi}(s,\mathfrak{f}) \sum_{H \in C(\mathfrak{H})} \chi(H),$$

the first sum taken over all characters of $\mathcal{O}_L(\mathfrak{f})/P(\mathfrak{f})$ and the second over the classes of the $\mathcal{O}$–free, proper modules.

6.2. Remark: One can express $F_{R,\chi}(s,\mathfrak{f})$ as a product over the prime ideals associated to the primary ideal decomposition of the conductor. It is meromorphic in s.

REFERENCES

[[**Ba**]] P. Bauer, *The Selberg Trace Formula for imaginary quadratic number fields of arbitrary class number*, Dissertation, to appear in: Bonner Math. Schriften (1990).

[[**B–Sh**]] Z.I. Borevich, I.R. Shafarevich, *Number Theory*, Academic Press, Inc., New York, San Francisco, London, 1966.

[[**Bou**]] N. Bourbaki, *Algèbre commutative, Chap. 1 à 4*, Masson, Paris, New York etc., 1985.

[[**Co**]] H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer–Verlag, New York, Berlin, Heidelberg, 1978.

[[**EGM**]] J. Elstrodt, F. Grunewald, J. Mennicke, *Eisenstein Series on Three–dimensional Hyperbolic Space and imaginary Quadratic Number Fields*, J. Reine und Angew. Math. **360** (1985), 160–213.

[[**Ha1**]] H. Hasse, *Vorlesungen über Klassenkörpertheorie*, Physica -Verlag, Würzburg, 1967.

[[**Ha2**]] H. Hasse, *Zahlbericht, 3. Auflage*, Physica -Verlag, Würzburg-Wien, 1970.

[[**Hi–Z**]] F. Hirzebruch, D. Zagier, *Intersection numbers of curves on Hilbert modular surfaces and modular forms of Nebentypus*, Inv. Math. **36** (1976), 57–113.

[[**Ka1**]] I. Kaplansky, *Composition of binary quadratic forms*, Studia Mathematica **31** (1968), 523–530.

[[**Ka2**]] I. Kaplansky, *Submodules of Quarternion Algebras*, Proc. Lond. Math. Soc. (3) **19** (1969), 219–232.

[[**L**]] E. Landau, *Elementary Number Theory*, Chelsea, New York, 1958.

[[**La1**]] S. Lang, *Algebraic Number Theory*, Addison–Wesley Publ. Co., Reading Mass., 1970.

[[**La2**]] S. Lang, *Elliptic Functions*, Addison–Wesley Publ. Co., Reading Mass., 1973.

[[**Mi**]] J. Milnor, *Introduction to Algebraic K–Theory*, AMS No. 72, Princeton Univ. Press, Princeton, 1971.

[[**Od**]] R.W.K. Odoni, *Representations of algebraic integers by binary quadratic forms and norm forms from full modules of extension fields*, J. Number Theory **10** (1978), 324–333.

[[**Oh**]] R. Ohta, *On Non–Maximal Orders of Algebraic Number Fields*, Nat. Sc. Rep., Ochanomizu Univ. **28**, **No. 1** (1977), 1–6.

[[**Sp**]] A. Speiser, *Die Theorie der binären quadratischen Formen mit Koefffizienten und Unbestimmten in einem beliebigen Zahlkörper*, Inaugural–Dissertation, Göttingen, 1909.

[[**St**]] E. Steinitz, *Rechteckige Systeme und Moduln in algebraischen Zahlkörpern. I.*, Math. Annalen **71** (1911–12), 328–354.

[[**v.d.W**]] B.L. van der Waerden, *Algebra, Zweiter Teil*, Springer–Verlag, Berlin, Heidelberg, New York, 1967.

[[**Z1**]] D.B. Zagier, *Zetafunktionen und quadratische Körper*, Springer–Verlag, Berlin, Heidelberg, New York, 1981.

[[**Z2**]] D.B. Zagier, *Modular forms whose coefficients involve Zeta functions of quadratic fields*, Int. Summer School on Modular Forms, Bonn (1976), 105–169.